PRIVACY IMPACT ASSESSMENT (PIA)

For the

Senior Leader Development Management System

Department of the Army, Senior Leader Development Office

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 7973 DA107171
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ **Yes**
- ☒ **No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0680-31a AHRC

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; and E.O. 9397, as amended (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

PRINCIPAL PURPOSE: To solicit and collect information from Army Competitive Category Colonels and General Officers for the purpose of career management and professional development.

DATA TYPES: Data maintained includes Social Security Number, name, grade, personal and family information, service, security clearance, assignment history, strength management data, civilian and military education, awards, training, branch and occupational specialties/areas of concentration, mailing addresses, telephone numbers, facsimile numbers, email addresses, physical location, languages, career pattern, performance, command and promotion history, retirement/separation information and service agreement information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The associated privacy risks with the PII collection are interception of transmitted data and unauthorized database access. Appropriate safeguards are in place for the collection and use of information, and we assess the risk to individuals' privacy as minimal. The system operates in a secure facility. Information assurance and security awareness training is administered to all users an annual basis. Access to data is restricted to individuals authorized access to the system as stated in the governing Privacy Act system notice. The Common Access Card (CAC) login is enforced. Hypertext Transfer Protocol Secure (HTTPS) is used with the Secure Sockets Layer (SSL) protocol for data in transit. Secure FTP (SFTP) is used for the transfer of data from other systems. SLDMS is a Tenant in Good Standing of the Headquarters Department of the Army Enterprise Network version 3.0 (HEN 3.0), its hosting environment. HEN 3.0 is certified and accredited at the MAC II SENSITIVE level by the DoD Information Assurance Certification and Accreditation Process (DIACAP).

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. U.S. Army Personnel Community, Army and Government Senior Leaders

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. United States Congress, Office of the POTUS

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. p 14 - This system is designed as a web-accessed data management system allowing for remote access with a CAC or password in compliance with Department of Defense and Department of the Army and HQDA access and security standards and specifications.

p. 22 - CYIOS Corporation: 5.1.6.8 Reportable Information Reporting. Design a

secure database for processing reportable information for senior officers. Reportable information is gathered from multiple agencies and prepared for review.

p. 22 - The contractor shall develop security policies and procedures for all information technology related issues for the SLD intranets/extranets and processes following quality control standards set forth by the COTR and IAW Army policies.

p. 22 - The contractor shall provide IT security for the SDL databases/network, develop a security policy, and coordinate with IMCEN for periodic upgrades to servers and the network to ensure secured access to data.

p. 22 - The contractor shall follow the guidelines of AR 25-2 to support systems certification and accreditation, password creation and usage standards, vulnerability scanning and other security measures to mitigate risk of the SLD network, systems, and users.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals (Military Officers) implicitly consent to capture and use of PII at the time of commissioning into the Armed Forces at which time they are provided a Privacy Advisory. However, individual may elect to opt out of providing some PII data elements that are not required for career management and development, including personal addresses, telephone numbers, email addresses and medical information.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Individual may elect to provide PII data elements that are not required for career management and development, including personal addresses, telephone numbers, email addresses and medical information, but restrict the release of that information any other persons or groups.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- ☒ **Privacy Act Statement**
- ☐ **Privacy Advisory**
- ☐ **Other**
- ☐ **None**

Describe each applicable format.

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C.; Public Law 104-134 (April 26, 1996)

PRINCIPAL PURPOSE(s): To solicit and collect information from Army Competitive Category Colonels and General Officers for the purpose of career management and professional development.

ROUTINE USE: The information gathered will be used for assignment, career management, and professional development purposes. Individual officers will have the ability to submit assignment preferences, as well as personal data relating to their careers. Human resource managers will use this information in the slating and development processes. Management reports will be used to review progress and slates at a macro level. All users' personally-identifiable information and actions while interacting with the information system will be collected and retained for information assurance purposes.

DISCLOSURE: Voluntary. Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish a social security number. This is an amendment to title 31, Section 7701. Furnishing the social security number, as well as other data, is voluntary, but failure to do so may delay or prevent action.